Symantec™ Client Security for Nokia® Communicator - Corporate Edition Implementation Guide

Symantec™ Client Security for Nokia® Communicator - Corporate Edition Implementation Guide

Documentation version: 3.0
PN: 10289274

Copyright Notice

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at wow-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information or device model number
- Available memory, disk space, NIC information
- Operating system or firmware revision
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC SOFTWARE LICENSE AGREEMENT
Symantec Client Security for Nokia Communicator

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use each copy of the Software, indicated in the License Module, on up to two computers and a single device as set forth in the documentation. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. use the Software in accordance with any written agreement between You and Symantec; and
E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;
B. use each licensed copy the Software on more than two computers, or for more than a single device without purchasing additional licenses;
C. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
D. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
E. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
F. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
G. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
H. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of thirty (30) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items,” as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec’s computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State’s Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

Technical support

Chapter 1 Introducing Symantec Client Security for Nokia Communicator - Corporate Edition

About Symantec Client Security 12
Components of Symantec Client Security 12
How Symantec Client Security works 14
    How the devices are protected 14
    How virus protection and Symantec Client Security are updated 15
    How activities are logged 16
What you can do with Symantec Client Security 16
Where to get more information 18

Chapter 2 Installing Symantec Client Security

System requirements 19
Installing the Symantec Client Security product 20
    Installing the Symantec Settings Builder administration tool 21
    Installing Symantec Client Security on the devices 21
Testing the installation 23
Uninstalling Symantec Client Security 23

Chapter 3 Protecting devices with Symantec Client Security

About scanning for and responding to viruses 25
    Auto-Protect scans 26
    Compressed file scans 26
    Expansion card scans 27
    Remote virus scans 27
About firewall protection 27
What to tell users about Symantec Client Security 28
About the Activity Log 28
    Virus-related activities 29
    Firewall-related activities 29
    When the log is full 30
Best practices for protecting devices 30

Chapter 4 Updating devices

About updating devices 31
LiveUpdate Wireless 32
What to tell users about updates 32
Initiating LiveUpdate Wireless remotely 33
Best practices for updating devices 33

Chapter 5 Initiating scans and updates remotely

About the Short Message Service (SMS) Listener 35
SMS message format 36
Using SMS messaging 36
About the command-line program 37
Initiating remote operations using SMS or the command-line program 38

Chapter 6 Configuring Symantec Client Security

About configuring Symantec Client Security 39
About the sample configuration file 40
Examining the ssb.ini file 40
About configuring Symantec AntiVirus and LiveUpdate Wireless 43
AV section parameters 43
LU section parameters 44
About configuring Symantec Client Firewall 46
Stateful inspection 47
FW section parameters 48
Incoming services 50
Outgoing services 52
FW.ICMPMsgs section 55
Using Symantec Settings Builder 59
Troubleshooting configuration files 60
Transferring configuration files to the devices 61
Required file locations 61
Configuration executables 61
Testing a new configuration 62
Best practices when configuring components 62

Index

Chapter 1

Introducing Symantec Client Security for Nokia Communicator - Corporate Edition

This chapter includes the following topics:

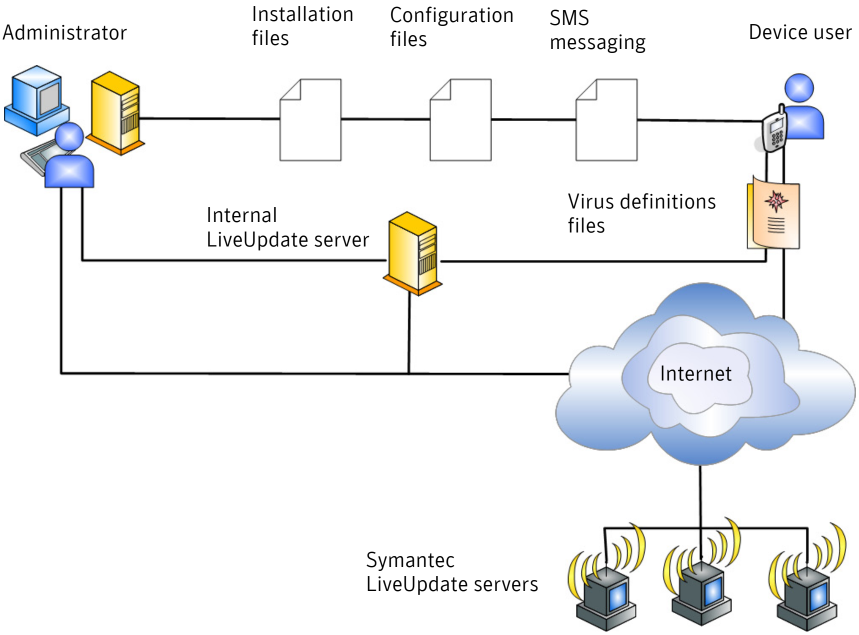
- About Symantec Client Security
- Components of Symantec Client Security
- How Symantec Client Security works
- What you can do with Symantec Client Security
- Where to get more information

This implementation guide is for administrators who manage multiple Nokia 9500 Communicators. It contains the information you need to install, update, and configure devices remotely.

To learn how to use the basic functions of Symantec Client Security on the Nokia 9500 Communicator, direct users to the context-sensitive Help and the Help file on the devices.

About Symantec Client Security

Symantec Client Security for Nokia Communicator - Corporate Edition provides secure mobile computing through comprehensive, reliable protection against malicious attacks directed at Nokia Communicators.



Components of Symantec Client Security

Table 1-1 lists and describes the components of Symantec Client Security.

Table 1-1 Symantec Client Security components

Component	What it does	Where it resides
Symantec Settings Builder administration tool	Enables administrators to create configuration files to set and lock antivirus and firewall parameters, and set LiveUpdate™ parameters on the devices. Administrators can transfer configuration files to the devices. See "Configuring Symantec Client Security" on page 39.	On the administrator's computer

Table 1-1 Symantec Client Security components

Component	What it does	Where it resides
Symantec AntiVirus™	Provides antivirus protection, and logs antivirus activities. Symantec AntiVirus is installed with Symantec Client Security. See "About scanning for and responding to viruses" on page 25. Administrators can remotely initiate interactive and non-interactive virus scans. See "Initiating scans and updates remotely" on page 35.	On the device
Symantec™ Client Firewall	Provides proactive network and application-level protection, and logs firewall activities. Symantec Client Firewall is installed with Symantec Client Security. See "About firewall protection" on page 27.	On the device
LiveUpdate Wireless	Allows users to update virus definitions files and Symantec products using an Internet connection. LiveUpdate Wireless obtains updates from the Symantec LiveUpdate server or an internal LiveUpdate server if configured by the administrator. LiveUpdate Wireless is installed with Symantec Client Security. See "Updating devices" on page 31. See "LiveUpdate Wireless configuration parameters" on page 44. Administrators can remotely initiate LiveUpdate Wireless sessions. See "Initiating scans and updates remotely" on page 35.	On the device

How Symantec Client Security works

The Symantec Client Security components work together to protect the devices from threats.

To understand how Symantec Client Security works, you need to know the following:

- How the devices are protected
- How virus protection and Symantec Client Security are updated
- How activities are logged

How the devices are protected

Symantec Client Security is an integrated security solution that combines antivirus and firewall protection for devices.

What happens when Symantec Client Security finds a virus

When Symantec Client Security identifies a suspicious file, either through Auto-Protect or an on-demand scan, it does the following:

- Blocks access to the file
- Displays a dialog that provides information about the potentially infected file and the option of deleting the file, repairing the file (if possible), or leaving the file as is
- Logs the found virus in the Activity Log
  See "About the Activity Log" on page 28.

Table 1-2 summarizes the types of virus scans that Symantec Client Security supports.

Table 1-2 Types of virus scans

Scan type	Description
Auto-Protect	Real-time scanning continuously inspects files as users access them on the devices. Real-time protection is enabled by default. Administrators can lock Auto-Protect on if they want to enforce a virus policy. Users cannot change any option that an administrator locks. See "Auto-Protect scans" on page 26.

Table 1-2 Types of virus scans

Scan type	Description
On-demand	On-demand (manual) scans inspect files and folders on the device and memory cards, and offer users the opportunity to delete, repair (if possible), or allow the file to remain as is. An administrator can remotely initiate interactive or non-interactive virus scans on the device. See "Remote virus scans" on page 27.

What happens when the firewall detects an unauthorized activity

When the Symantec Client Security firewall detects an unauthorized activity such as blocked inbound or outbound connections or port scanning attempts, it does the following:

- Displays a dialog that provides information about the unauthorized activity
- Logs the firewall activity in the Activity Log
  See "About the Activity Log" on page 28.

How virus protection and Symantec Client Security are updated

Symantec™ Security Response provides administrators and users with regular updates to virus definitions files to keep their virus protection current. In addition, Symantec may also provide software updates to Symantec Client Security.

Symantec Client Security offers the following methods of obtaining updates:

LiveUpdate Wireless directly from the Symantec LiveUpdate server	Symantec Client Security can use LiveUpdate Wireless to connect to the Symantec LiveUpdate server and obtain virus definitions files and product updates the next time that the device connects to the Internet. Users can initiate updates on the devices or administrators can initiate updates remotely.
LiveUpdate Wireless using an internal LiveUpdate server	LiveUpdate Wireless on the device can pull virus definitions files and product updates from an internal LiveUpdate server the next time that the device connects to the network. Administrators can configure this update method.

See "LiveUpdate Wireless" on page 32.

How activities are logged

The Symantec Client Security software on the device records information about the following actions that are performed on the device:

Antivirus activities	■ Partial and full virus scans ■ Viruses found ■ Repaired files ■ Infected files deleted ■ Infected files not deleted
Firewall activities	■ Blocked outbound TCP connections ■ Blocked inbound TCP connections ■ Port scanning attempts (suspicious network activity, which may be a port scan)

Users can view this data directly on the device.

See “About the Activity Log” on page 28.

What you can do with Symantec Client Security

You can do the following with Symantec Client Security:

Protect the devices with real-time and on-demand scanning for viruses.	Symantec Client Security provides antivirus protection for the devices on which it runs. Auto-Protect monitors activity on the device and looks for viruses when users open, run, rename, or move files, or copy files to and from folders. Users can initiate on-demand scans that systematically check the files on the device for viruses. Administrators can initiate remote scans on the devices. See “About scanning for and responding to viruses” on page 25.
Protect the devices with centralized firewall management.	Symantec Client Security provides firewall protection for the devices on which it runs. Centralized firewall management lets you create and modify firewall policy files, and then push them to the devices. See “About firewall protection” on page 27.

Update virus protection.	Symantec Client Security employs virus definitions files to detect known Symbian OS™ viruses. Symantec makes updated virus definitions files available regularly. For Nokia Communicators, LiveUpdate Wireless can obtain the latest virus definitions and product updates over the Internet. See “Updating devices” on page 31.
Monitor antivirus activity.	The Activity Log on the device provides key information about antivirus activities, including partial scans, full scans, found viruses, repaired files, deleted infected files, and failures to delete infected files. See “About the Activity Log” on page 28.
Monitor intrusion attempts.	The Activity Log on the device provides key information about firewall activities, including blocked outbound TCP connections, blocked inbound TCP connections, and port scanning attempts (suspicious network activity, which may be a port scan). See “About the Activity Log” on page 28.
Centrally update and configure multiple devices.	Administrators use their existing infrastructure to transfer update and configuration files to multiple devices, and to remotely initiate product and virus definitions updates and virus scans. See “Configuring Symantec Client Security” on page 39. See “Initiating scans and updates remotely” on page 35.

Where to get more information

This *Symantec Client Security for Nokia Communicator - Corporate Edition Implementation Guide* for administrators is available in PDF format on the product CD in the following location:

Manual\scs_nokia_imp.pdf

A printed version of this guide is also included.

User documentation is provided on the devices in the form of context-sensitive Help and the Help file.

For late-breaking news, read the Readme.txt file, which is located in the root directory on the CD.

Table 1-3 lists Symantec Web sites that provide additional information.

Table 1-3 Symantec Web sites

Types of information	Web address
Public Knowledge Base Releases and updates Manuals and documentation Contact options	http://www.symantec.com/techsupp/enterprise/
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Platinum Support Web access	https://www-secure.symantec.com/platinum/

Chapter 2

Installing Symantec Client Security

This chapter includes the following topics:

- System requirements
- Installing the Symantec Client Security product
- Testing the installation
- Uninstalling Symantec Client Security

System requirements

If you plan to push the installation files from a computer that uses mobile device management software, you need to install Nokia PC Suite in addition to the mobile device management software.

Install Symantec Settings Builder on the computer from which you plan to push configuration files to the devices.

Table 2-1 lists the system requirements for copying files from the CD and for using the Symantec Settings Builder administration tool.

Table 2-1 CD Start and Symantec Settings Builder system requirements

Operating system	Requirements
Windows NT® 4.0 Workstation/Server with Service Pack 6a	■ Pentium 100 MHz ■ 58 MB of RAM
Windows 2000 Server™/Advanced Server/ Professional with Service Pack 2 Windows® XP Professional with Service Pack 2 Windows 2003 .NET Server	■ Pentium 233 MHz with MMX ■ 58 MB of RAM

Table 2-2 lists the system requirements for the devices.

Table 2-2 Device requirements

Operating system or component	Requirements
Symbian OS	■ Installation footprint: 300 KB ■ Nokia Communicator 9500 or other series 80 platform 2.0 compatible device
LiveUpdate Wireless	Internet connection

Installing the Symantec Client Security product

To install Symantec Client Security, you must perform the following tasks:

- Install the Symantec Client Security Symantec Settings Builder administration tool on the administrator's computer.
  See "Installing the Symantec Settings Builder administration tool" on page 21.
- Install Symantec Client Security on the devices.
  See "Installing Symantec Client Security on the devices" on page 21.

Installing the Symantec Settings Builder administration tool

You need to copy the Symantec Settings Builder administration tool files to the computer that hosts your existing infrastructure for pushing configuration files and updates.

To install the Symantec Settings Builder administration tool

1. Insert the Symantec Client Security CD into the CD-ROM drive.
2. Click **Browse CD**.
3. From the Tools folder, copy the following files to any directory on the computer:
   - ssb.exe
   - ssb.ini

See "Configuring Symantec Client Security" on page 39.

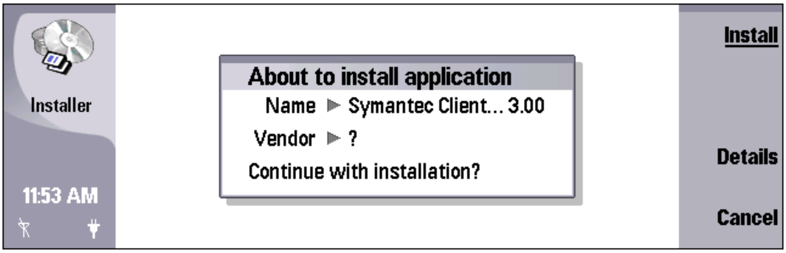
Installing Symantec Client Security on the devices

You need to copy the installation (.sis) file to the devices and run it.

To install Symantec Client Security on the devices

1. Insert the Symantec Client Security CD into the CD-ROM drive of the computer that will push the installation.
2. Click **Browse CD**.
3. From the root directory, copy the SymCS_S80_70s_corp_AM.sis file into the location from which you usually push files to your devices.
4. Place the .sis file onto the devices. For example, you might do one of the following:
   - Configure the existing infrastructure from which you push installation files to put the .sis file into any location on the devices.
   - Place the memory card that contains the .sis file into each of the devices, and then copy the .sis file into any location on the devices.

5. After the .sis file is on the devices, run it. For example, you might do one of the following:
   - Configure the existing infrastructure from which you push installation files to run the .sis file remotely.
   - Run the .sis file, or have your users run the .sis file on each of the devices.



About to install application

Name ▶ Symantec Client... 3.00

Vendor ▶ ?

Continue with installation?

6. Users must then follow the on-screen instructions to complete the installation.
   An icon for Symantec Client Security appears on the Desk after installation is complete.

If you need to reinstall

The installation may fail if one or more files are missing or corrupted, or if the device has been reset.

To reinstall Symantec Client Security

1. Uninstall Symantec Client Security.
   See “Uninstalling Symantec Client Security” on page 23.
2. Ensure that the following Symantec files are removed:
   - C:\System\Apps\SymCS\ directory and its contents
   - C:\System\Apps\SymLU\ directory and its contents
   - C:\System\Help\Sym*.* files
   - C:\System\Libs\Sym*.* files

   The on-device File Manager displays Communicator rather than C: in the file hierarchy.
   If the System folder does not appear in the file hierarchy, configure File Manager to display it.
3. Reinstall using the standard installation procedure.
   See “Installing the Symantec Client Security product” on page 20.

Testing the installation

You can verify that Symantec Client Security is active by downloading the standard European Institute for Computer Anti-Virus Research (EICAR) test file, and copying it to the device.

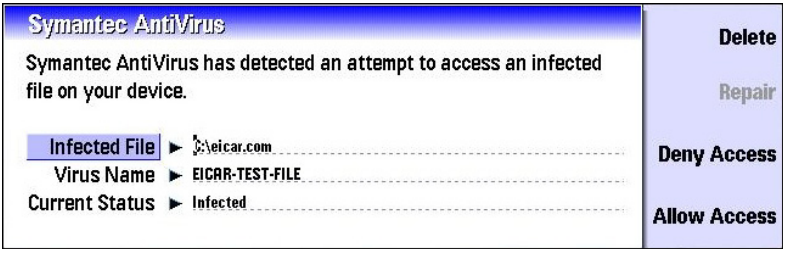
To test the installation

1. Download the EICAR test file from www.eicar.org

   You may need to turn off virus scanning on the administrator's computer temporarily to access the EICAR test file. Make sure that you turn on virus scanning on the administrator's computer after you are finished.

2. Copy the EICAR test file to the device and open it.

   If the installation of Symantec Client Security is successful, a dialog appears.



Symantec AntiVirus

Symantec AntiVirus has detected an attempt to access an infected file on your device.

Infected File ► C:\eicar.com
Virus Name ► EICAR-TEST-FILE
Current Status ► Infected

Uninstalling Symantec Client Security

To uninstall Symantec Client Security, you must remove the Symantec Settings Builder administration tool from the administrator's computer, and then remove the Symantec Client Security files from the devices.

To uninstall the Symantec Settings Builder administration tool files

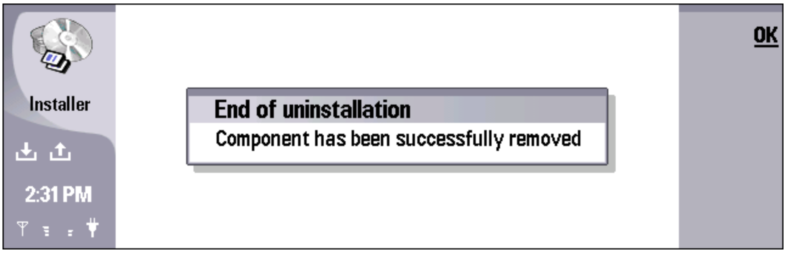
1. Locate and delete the following Symantec Settings Builder files:
   - ssb.exe
   - ssb.ini
2. Locate and delete any .cfg files that the tool generated.

   The .cfg files are located in the same directory as the ssb.exe and ssb.ini files, by default.

To uninstall Symantec Client Security on the devices

1 In the Desk view, select **Tools** > **Control panel** > **Data management** > **Application manager.**

2 In the Application manager view, on the Installed software page, select **Symantec Client Security** > **Remove**.



End of uninstallation

Component has been successfully removed

Chapter 3

Protecting devices with Symantec Client Security

This chapter includes the following topics:

- About scanning for and responding to viruses
- About firewall protection
- What to tell users about Symantec Client Security
- About the Activity Log
- Best practices for protecting devices

About scanning for and responding to viruses

To understand how scanning works, you need to know about the following types of scans:

- Auto-Protect scans
- Compressed file scans
- Expansion card scans
- Remote virus scans

Administrators can configure and lock scan settings using a configuration file that is pushed to the devices.

See “Configuring Symantec Client Security” on page 39.

Auto-Protect scans

As users access files on the devices, Auto-Protect provides real-time virus scanning. Although infected files, including email messages or expansion card files, could be stored on the device, these files are checked when users attempt to open them. Auto-Protect scans all of the files on expansion cards only after users initiate an on-demand scan.

When Auto-Protect scans a suspicious file, it blocks access to the file and presents a dialog that lets users do the following:

Repair	This action attempts to repair the infected file.
Delete	This action deletes the infected file and is the recommended action.
Deny Access	This action does not open the infected file and stops the current activity to prevent users from using an infected file.
Allow	This action continues the current activity. Users select this action only if they are sure that a virus is not at work. Users will receive an alert each time that they open the file.

Auto-Protect implements a file name-based cache to minimize performance impact.

Note: If the Auto-Protect setting on the device is not locked by the administrator, users can turn off Auto-Protect, even if it is turned on by the administrator in the configuration file.

Compressed file scans

Compressed files (for example, .sis, .jar, and .zip files) may contain infected files. When users open a compressed file, the files that it contains are not scanned by Auto-Protect until they are extracted and then accessed.

Users must extract and scan all files; repair the infected files; and if possible, delete and recreate the compressed file.

When users initiate on-demand scans, the files inside a compressed file are extracted and scanned. If there is not enough space on the Communicator drive to extract an individual file in the archive, that file is skipped during the scan of the archive. However, users are still protected if Auto-Protect is enabled. When the skipped files are accessed after extraction, Auto-Protect will scan the files.

Expansion card scans

Symantec Client Security does not scan newly inserted expansion cards. Users must manually initiate a scan after inserting an expansion card.

Administrators can remotely initiate a scan of expansion cards using Short Message Service (SMS) messages.

See "Initiating scans and updates remotely" on page 35.

Remote virus scans

The administrator can initiate interactive and non-interactive virus scans on a device remotely.

See "Initiating scans and updates remotely" on page 35.

About firewall protection

You can create and manage firewall policies that are as restrictive or permissive as necessary to control access to and from devices.

See "About configuring Symantec Client Firewall" on page 46.

The firewall is enabled by default, with the protection level set to Medium.

Table 3-1 describes the default protection level settings.

Table 3-1 Default protection level settings

Parameter	Default setting
LocalTrafficAllowed	Set to allow local traffic
IGMPAllowed	Set to disallow all IGMP messages
TrafficNotifications	Set to issue no notifications
Inbound connections	None are allowed
Outbound connections	All are allowed
ICMP Echo Request	Set to AllowOutgoing
Echo Reply	Set to AllowIncoming
Packet Too Big	Set to AllowIncoming

What to tell users about Symantec Client Security

Information that you may want to give users about how Symantec Client Security functions and what may happen on their devices based on your configuration of the software include the following:

Symantec AntiVirus

- If the administrator has locked antivirus settings, these settings appear dimmed on the devices, and cannot be changed by the users.
- The administrator can initiate remote interactive and non-interactive scans. Interactive scans require users to delete or repair any infected files.
- If the administrator initiates a remote interactive scan, a dialog appears that displays all of the files that are being scanned.
- Users should initiate an on-demand scan any time that they think that the device may contain a virus. On-demand scans are particularly important if users have ever disabled Auto-Protect on the device.
- Auto-Protect does not automatically scan expansion cards. However, if users attempt to access an infected file on an expansion card, Auto-Protect will detect the infected file.
- Any time users insert an expansion card, they should initiate an on-demand scan.

See “About configuring Symantec Client Security” on page 39.

Symantec Client Firewall

- If the administrator has locked firewall settings, these settings appear dimmed on the devices, and cannot be changed by the users.
- Firewall settings may interfere with the normal operation of some applications. For example, setting the protection level to High will severely restrict traffic.

See “About configuring Symantec Client Firewall” on page 46.

About the Activity Log

The device maintains a local history of antivirus and firewall activity. The following activities can be viewed only from the device:

- Virus-related activities
- Firewall-related activities

Virus-related activities

The following virus-related activities are recorded by the device:

Partial scan	A partial scan entry is added when users cancel a scan, or scan only part of the device (for example, only the device's main memory, and not its expansion card).
Full scan	A full scan entry is added when the entire device, including any expansion cards, is scanned.
Found virus	A found virus entry is added whenever Symantec Client Security identifies a file that is infected with a virus. Included in this entry is the action that was taken on the infected file.

Firewall-related activities

The following firewall-related activities are recorded by the device:

Blocked outbound TCP connection	An entry is added when a blocked outbound TCP connection is attempted.
Blocked inbound TCP connection	An entry is added when a blocked inbound TCP connection is attempted.
Port scanning attempt	An entry is added when port scanning is attempted.

For each firewall-related activity, the log provides the following details:

- Date of occurrence
- Time of occurrence
- Protocol involved (TCP only)
- Direction (Outbound/Inbound)
- Source IP address
- Source port
- Destination IP address
- Destination port

Note: The amount of firewall log entries within a specified time interval is limited. If there are a large number of events in a short time, only a subset of these events will be logged.

When the log is full

When the Activity Log reaches 100 KB in size, Symantec Client Security first compacts the log file, which usually frees up a lot of space. If compacting the log file does not free up enough space, entries are deleted (oldest first) until the size drops below 100 KB. Users can also delete individual log entries or clear the entire log to keep it from using too much memory.

Best practices for protecting devices

The best practices for protecting devices are as follows:

- Run LiveUpdate regularly to get the latest virus definitions.
- Scan the devices regularly with the latest virus definitions.
- Keep Auto-Protect enabled.
- Keep the firewall enabled, with the protection level set to at least Medium.
- Ask users to pay attention to warnings that appear during the installation of other applications, such as invalid certificates, unknown vendors, and so on, and make sure that you trust the source before continuing with the installation.
- Enforce a password policy. Using complex passwords helps to prevent or limit damage when a device is compromised.
- If you don’t already have antivirus software on your email server, you should configure your email server to block or remove messages that contain file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr files.
- Isolate infected devices quickly to prevent compromising your organization further. Perform a forensic analysis and restore the devices using trusted media.
- Instruct users not to open attachments unless they are expecting them. If Auto-Protect is disabled, users should not run software that they download from the Internet unless it has been scanned for viruses.

Updating devices

This chapter includes the following topics:

- About updating devices
- What to tell users about updates
- Initiating LiveUpdate Wireless remotely
- Best practices for updating devices

About updating devices

Symantec Client Security supports the following types of updates:

Virus definitions file updates	Symantec products use virus definitions files to identify viruses. Symantec Security Response researches and responds to new virus threats and provides customers with updates of virus definitions files as new viruses emerge.
Software updates	Symantec occasionally provides software patches to Symantec products.
Engine updates	Symantec occasionally provides antivirus scan engine updates to take into account new types of threats that have been identified.

LiveUpdate Wireless

Administrators and users can access Symantec Client Security updates by using LiveUpdate Wireless. Table 4-1 lists and describes each update method.

Table 4-1 Possible update methods

Method	How it works	When to use it
LiveUpdate Wireless using the HTTP protocol on the Internet	A pull operation initiated by the device users or a push operation initiated by the administrator on a device on which LiveUpdate Wireless is being used. LiveUpdate Wireless downloads the update directly from the Symantec LiveUpdate server.	Use this method when you want updates to come directly from Symantec.
LiveUpdate Wireless using an internal server	A pull operation initiated by the device users or a push operation initiated by the administrator on a device on which LiveUpdate Wireless is being used. LiveUpdate Wireless requests the update directly from an internal LiveUpdate server that is configured by an administrator.	Use this method when you want to control the updates that the devices can retrieve.

Information about setting up an internal LiveUpdate server is located in the *LiveUpdate Administrator's Guide*. The guide is available on the Symantec Support Web site:

http://www.symantec.com/techsupp/files/lu/lu.html

What to tell users about updates

Users need to know that when they update certain products, they may need to turn their phones off and then on again for the update to take effect. If this occurs, they will see a dialog that tells them what to do.

If you want your users to use an HTTP proxy for LiveUpdate Wireless, you need to tell them the address and port to use, and the user name and password that is required for authentication, if necessary. Because proxy settings are set through the Symbian OS software and not through Symantec Client Security, users should refer to their Symbian documentation for information about how to add these settings.

Initiating LiveUpdate Wireless remotely

You can initiate a search for virus definitions files and product updates on the devices.

See “Initiating scans and updates remotely” on page 35.

Best practices for updating devices

Update devices with the latest virus definitions files and product updates regularly.

Initiating scans and updates remotely

This chapter includes the following topics:

- About the Short Message Service (SMS) Listener
- About the command-line program
- Initiating remote operations using SMS or the command-line program

About the Short Message Service (SMS) Listener

The Short Message Service is available on many digital-based mobile communications systems. An SMS message is usually 140 to 160 characters long, with each character 7 or 8 bits in length. SMS messages can be sent and received in either text mode or Protocol Description Unit (PDU) mode. If the device is not on or is out of range, messages can be stored in the network and delivered when the device is next available.

The SMS Listener that is installed on the device as part of Symantec Client Security is a background process that listens on a Symantec private port (57319) for incoming binary SMS messages. An SMS message sent to this port can be used to initiate interactive or non-interactive virus scans, or to initiate LiveUpdate Wireless to update virus definitions and product software on a device.

SMS Listener can be enabled or disabled using a Symantec Settings Builder configuration file.

See Table 6-3, “Antivirus configuration parameters,” on page 43.

SMS message format

SMS messages that are sent to SMS Listener must be in PDU mode. The SMS messages that you send should use the following characteristics:

Protocol Identifier (TP-PID)

Protocol ID subgroup: SME interworking, SME-to-SME protocol

Data Coding Scheme (TP-DCS)

Coding Group: Coding/Message class

Alphabet: 8-bit data

Message Class: Class 1 ME-specific

Application Port Addressing

Create port addressing field: Destination port 57319

Using SMS messaging

The Symantec SMS message payload format is as follows:

CommandIDTotalLengthData

Table 5-1 describes each of the message payload fields.

Table 5-1 Message payload fields

Field	Length	Description
CommandID	2 bytes	The action to be taken when the message is received. Defined CommandIDs are as follows: ■ 0: Perform a silent search for updates to all products and virus definitions. ■ 1: Start the Symantec AntiVirus user interface to scan for viruses interactively. ■ 2: Start the Symantec AntiVirus user interface to scan for viruses without interaction.
TotalLength	2 bytes	TotalLength is the length of the entire payload, in bytes.
Data	N bytes This field is optional.	The final field can be present or not, depending on the value of the CommandID field. Currently, the Data field is reserved for future use.

Note: The binary SMS payload sent by some software programs must have the byte order of every two- and four- byte quantity reversed.

Some sample payloads are shown in Table 5-2.

Table 5-2 Sample payloads

Sample payload	What this payload does
00000004	Initiates a silent update of all products and virus definitions
00020004	Initiates a non-interactive virus scan
00000400	Initiates a silent update of all products and virus definitions (byte order reversed)
02000400	Initiates a non-interactive virus scan (byte order reversed)

To use SMS messaging

1. Prepare the appropriate binary SMS payload.
2. Configure the software that you are using to send the binary SMS message using the SMS message format information that is provided.
   Ensure that you send the message to destination port 57319.
3. Use your software to send the message.

About the command-line program

A command-line program is installed on the device as part of Symantec Client Security. This program can be used by other programs to initiate interactive or non-interactive virus scans, or to initiate LiveUpdate Wireless to update virus definitions and product software on the device.

This command-line program is designed to be run from another program, such as a local script prepared for use with mobile device management software, so that it can pass command-line arguments that specify the command to run. If the command-line program is run without arguments (for example, from the Symbian user interface using the File Manager), it does nothing.

The command-line program has one argument, the CommandID, which is a required keyword that specifies the command to run. The CommandIDs are as follows:

SUPDALL	Silent update of all installed products and virus definitions files
ISCAN	Interactive scan of the device
SSCAN	Non-interactive (silent) scan of the device

Initiating remote operations using SMS or the command-line program

Using the defined CommandIDs for SMS messages or the command-line program, you can initiate a search for virus definitions files and product updates, and interactive and non-interactive virus scans on the devices.

You can use any program that is available to you that allows you to send binary SMS messages. When using the command-line program, you can use any available program that can run the command-line program.

If you use one of these methods to initiate an update, and one or more products or the virus definitions are updated, a message that says “Symantec products updated” is displayed on the device until the user dismisses it.

If an update requires that the phone be turned off and then on again, a message that says “Symantec products updated - phone restart required” is displayed on the device until the user dismisses it.

If an interactive scan discovers a virus, users are prompted to delete the file or repair it (if possible).

Note: If device reception is inadequate, an update may fail silently, and you will need to initiate it again.

Chapter 6

Configuring Symantec Client Security

This chapter includes the following topics:

- About configuring Symantec Client Security
- About the sample configuration file
- About configuring Symantec Client Firewall
- Using Symantec Settings Builder
- Transferring configuration files to the devices
- Testing a new configuration
- Best practices when configuring components

About configuring Symantec Client Security

Symantec Client Security provides the Symantec Settings Builder administration tool for the wireless configuration of the product that is running on Nokia Communicators. Symantec Settings Builder is a command-line tool that lets administrators create configuration files to set and lock Symantec AntiVirus and Symantec Client Firewall parameters, and to set LiveUpdate Wireless parameters on the devices. The administrator can distribute files to devices using their existing infrastructure to transfer update and configuration files.

About the sample configuration file

The Symantec Settings Builder executable takes a file in the standard Windows .ini file format as input. The sample input file that is provided with Symantec Settings Builder is named ssb.ini.

To configure devices remotely, you need to do the following:

- Copy and rename the ssb.ini file.
- Edit your copy of this input configuration file to set the Symantec AntiVirus, LiveUpdate Wireless, and Symantec Client Firewall configuration parameters that you want.
- Use Symantec Settings Builder to package these settings into configuration (.cfg) files that you can distribute to your devices.

Depending on how you edit your input configuration file, Symantec Settings Builder produces one or more of the following files:

av.cfg	Symantec AntiVirus configuration file for the Nokia Communicator
lu.cfg	LiveUpdate Wireless configuration file for the Nokia Communicator
fw.cfg	Symantec Client Firewall configuration file for the Nokia Communicator

By default, Symantec Settings Builder creates all the .cfg files in the order given. The files are placed in the current directory of your computer by default, but you can specify another location for them by setting the OutputDir parameter in your input file.

Examining the ssb.ini file

The ssb.ini file is annotated with comments that explain the various parameters and how to set them. You should open and look at the ssb.ini file while following the complete reference to the file contents that is provided here.

The file is divided into the sections that are shown in Table 6-1. A summary of the section parameters is provided in the tables that are noted.

Table 6-1 ssb.ini sections

ssb.ini section	Description	Files affected
[SSB]	Application operation parameters See Table 6-2.	All files

Table 6-1 ssb.ini sections

ssb.ini section	Description	Files affected
[AV]	Symantec AntiVirus configuration parameters See Table 6-3.	av.cfg
[LU]	LiveUpdate Wireless configuration parameters See Table 6-4.	lu.cfg
[FW]	General Symantec Client Firewall configuration parameters See Table 6-5.	fw.cfg
[FW.IncomingSvcs]	Incoming user-defined services for custom firewall parameters See the following: ■ Table 6-6, User-defined incoming services count parameter ■ Table 6-7, User-defined incoming services entry format ■ Table 6-8, User-defined incoming services sample entries	fw.cfg
[FW.InStdSvcs]	Incoming standard services for custom firewall parameters See the following: ■ Table 6-9, Standard incoming services count parameter ■ Table 6-10, Standard incoming services entry format ■ Table 6-11, Standard incoming services sample entries	fw.cfg
[FW.OutgoingSvcs]	Outgoing user-defined services for custom firewall parameters See the following: ■ Table 6-12, User-defined outgoing services count parameter ■ Table 6-13, User-defined outgoing services entry format ■ Table 6-14, User-defined outgoing services sample entries	fw.cfg

Table 6-1 ssb.ini sections

ssb.ini section	Description	Files affected
[FW.OutStdSvcs]	Outgoing standard services for custom firewall parameters See the following: ■ Table 6-15, Standard outgoing services count parameter ■ Table 6-16, Standard outgoing services entry format ■ Table 6-17, Standard outgoing services sample entries	fw.cfg
[FW.ICMPMsgs]	ICMP message types for custom firewall parameters See the following: ■ Table 6-18, ICMP message types count parameter ■ Table 6-19, ICMP message types format ■ Table 6-20, ICMP message types sample entries ■ Table 6-21, ICMP message types values	fw.cfg

SSB section parameters

Table 6-2 describes the application operation parameters in the ssb.ini file.

Table 6-2 Application operation parameters

SSB section parameter	Description
Verbose=<value>	Determines the level of verboseness Symantec Settings Builder produces, where <value> is one of the following: ■ 0: This turns off verbose mode. ■ 1: This turns on verbose mode so that Symantec Settings Builder shows progress and parameter values on the console when it runs. Note: Validation error messages are sent to standard error output when you run Symantec Settings Builder, regardless of whether the Verbose parameter is set to 1. The default setting is 0 (disabled).

Table 6-2 Application operation parameters

SSB section parameter	Description
OutputDir=<path>	The location where the .cfg files are generated. If the directories do not exist, they will be created. The directory part of the path must end with a backslash (\). The default is the current directory (.\).

About configuring Symantec AntiVirus and LiveUpdate Wireless

You can configure Symantec AntiVirus and LiveUpdate Wireless settings by pushing configuration files to the devices. Users can configure settings on the devices if the settings are not locked.

When you push new configuration files for Symantec AntiVirus ([AV] section) and LiveUpdate Wireless ([LU] section), the settings in the new file completely overwrite the current settings on the device. Any parameter that is not explicitly set in the configuration files reverts to its default value.

AV section parameters

Table 6-3 describes the Symantec AntiVirus configuration parameters in the ssb.ini file.

Table 6-3 Antivirus configuration parameters

AV section parameter	Description
Create=<value>	Determines whether a file is produced for Symantec AntiVirus configuration settings, where <value> is one of the following: ■ 0: This does not produce a file for Symantec AntiVirus settings. ■ 1: This creates an av.cfg file with Symantec AntiVirus settings. The default is 1 (create Symantec AntiVirus settings).
AutoProtect=<value>	Determines whether AutoProtect is enabled, where <value> is one of the following: ■ 0: This disables AutoProtect. ■ 1: This enables AutoProtect. The default is 1 (enabled).

Table 6-3 Antivirus configuration parameters

AV section parameter	Description
LockAutoProtect=<value>	Determines whether users can change the Auto-Protect setting on the device, where <value> is one of the following: ■ 0: This enables users to change the setting on the device. ■ 1: This prevents users from changing the setting on the device. The Auto-Protect user interface on the device is locked. The default is 0 (allow user change).
EnableSMSListener=<value>	Enables the SMS Listener program installed on the device, where <value> is one of the following: ■ 0: This disables the SMS Listener. ■ 1: This enables the SMS Listener. The default is 1 (enabled). See "About the Short Message Service (SMS) Listener" on page 35.

LU section parameters

Table 6-4 describes the LiveUpdate Wireless parameters in the ssb.ini file.

Table 6-4 LiveUpdate Wireless configuration parameters

LU section parameter	Description
Create=<value>	Determines whether a file is produced for LiveUpdate Wireless configuration settings, where <value> is one of the following: ■ 0: This does not produce a file for LiveUpdate Wireless settings. ■ 1: This creates an lu.cfg file with LiveUpdate Wireless settings. The default is 1 (create LiveUpdate Wireless settings).
Enabled=<value>	Determines whether LiveUpdate Wireless is enabled, where <value> is one of the following: ■ 0: This disables LiveUpdate Wireless. ■ 1: This enables LiveUpdate Wireless. The default is 1 (enabled).

Table 6-4 LiveUpdate Wireless configuration parameters

LU section parameter	Description
UseInternal=<value>	Determines whether LiveUpdate Wireless uses an internal LiveUpdate server or the Symantec LiveUpdate server, where <value> is one of the following: ■ 0: This disables the use of an internal LiveUpdate server. The Symantec LiveUpdate server will be used. ■ 1: This enables the use of an internal LiveUpdate server. Use an internal server if you want to control the updates users can access. The default is 0 (disabled). See "LiveUpdate Wireless" on page 32.
InternalURL=<URL>	Sets the URL of the internal LiveUpdate server that you want to use. This parameter can be specified with an IP address in the following format: http://111.222.333.444/ The maximum number of characters that are allowed in the URL is 255. If UseInternal is set to 1, this parameter is mandatory. If UseInternal is set to 1 and this parameter is not set, a validation error is sent to standard error output. There is no default.

About configuring Symantec Client Firewall

You can configure Symantec Client Firewall settings by pushing configuration files to the devices. Users can configure settings on the devices if the settings are not locked.

When you are configuring firewall settings, keep in mind the following considerations:

- This implementation of Symantec Client Firewall stops all TCP/IP network traffic that is not specifically enabled or allowed by its configuration settings.
- If you plan to configure your own custom settings for the Symantec Client Firewall, you must set the ProtectionLevel parameter to 3.
- When you push new configurations for Symantec Client Firewall using the custom ProtectionLevel (parameter value of 3), any parameter that is not explicitly set in the configuration files takes its predefined value for that protection level. The only exceptions are the enabled and locked parameters. If you set the ProtectionLevel parameter to 0, 1, or 2, and you also set values in the input file for LocalTrafficAllowed, IGMPAllowed, and TrafficNotifications, the predefined values are used and the values that you set explicitly in the file for LocalTrafficAllowed, IGMPAllowed, and TrafficNotifications are ignored.
- When you use the custom firewall configuration features (ProtectionLevel set to 3), you can configure the firewall incrementally. If a setting is not changed by the new configuration file, it remains in force on the device until it is either explicitly changed by a new configuration file or it is changed on the device through the user interface. For example, if you have previously set the device to allow all Telnet traffic, and you push a configuration file that sets the device to allow only SMTP traffic, the device subsequently allows all Telnet and SMTP traffic.
- If you configure the firewall settings of your devices by pushing a configuration file, the only way to take firewall entries out of the user interface on the device is to set their state to Delete.
- To return to a default state for firewall settings, you can set the ProtectionLevel parameter to 1 (Medium) and push that firewall configuration file to the devices.

Stateful inspection

The firewall uses stateful inspection, a process that creates a connection state table that tracks information about current connections such as source and destination IP addresses, ports, and applications. For example, if a firewall rule permits a client to connect to a Web server, the firewall logs connection information in the state table. When the server replies, the firewall checks the state table, discovers that a response from the Web server to the client is expected, and permits the Web server traffic to flow to the initiating client without inspecting the rulebase. A rule must permit the initial outbound traffic before the firewall logs the connection in the state table.

Stateful inspection allows you to simplify your firewall configuration because you don't have to create rules that permit traffic in both directions for traffic typically initiated in one direction only. Client traffic typically initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443, encrypted Web traffic). These are preset for you as standard services. Clients initiate this traffic outbound so you only have to create a rule that permits outbound traffic for these protocols. The firewall permits the return traffic when it inspects the state table.

By configuring outbound rules only, when possible, you increase client security in the following ways:

- Reduce rulebase complexity.
- Eliminate the possibility that a worm or other malicious program can initiate connections to a client on ports configured for outbound traffic only. You can also configure inbound rules only, for traffic to clients that clients do not initiate.

Stateful inspection supports all rules that direct TCP/UDP traffic. Stateful inspection does not support rules that filter ICMP traffic. For ICMP, you must create rules that permit traffic in both directions when necessary. For example, if you want clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

FW section parameters

Table 6-5 describes the general firewall parameters in the ssb.ini sample file that you can configure using Symantec Settings Builder.

Table 6-5 Symantec Client Firewall general configuration parameters

FW section parameter	Description
Create=<value>	Determines whether a file is produced for Symantec Client Firewall configuration settings, where <value> is one of the following: ■ 0: This does not produce a file for firewall settings. ■ 1: This outputs firewall settings to the fw.cfg file. The default is 1 (create firewall settings).
Enabled=<value>	Determines whether the Symantec Client Firewall is enabled, where <value> is one of the following: ■ 0: This disables the firewall. ■ 1: This enables the firewall. The default is 1 (enabled).
LocalTrafficAllowed=<value>	Determines whether local traffic is allowed by Symantec Client Firewall. Local traffic (loopback) is TCP/IP traffic that is moving between the applications that are running on the devices. <value> is one of the following: ■ 0: This does not allow local traffic. ■ 1: This allows local traffic. The default is 1 (allow local traffic). If you know that your devices do not require local traffic, disallowing it prevents malicious applications from exploiting this type of communication.
IGMPAllowed=<value>	Determines whether IGMP traffic is allowed by Symantec Client Firewall. IGMP is commonly used to send multimedia files to multicast groups. <value> is one of the following: ■ 0: This does not allow IGMP traffic. ■ 1: This allows IGMP traffic. The default is 1 (allow IGMP traffic).

Table 6-5 Symantec Client Firewall general configuration parameters

FW section parameter	Description
TrafficNotifications=<value>	Determines whether the firewall sends traffic notifications to the device user interface. Traffic notifications are short messages that appear briefly on the device when a Symantec Client Firewall rule blocks traffic. <value> must be one of the following: ■ 0: This sends no notifications. ■ 1: This sends notifications about incoming traffic. ■ 2: This sends notifications about outgoing traffic. ■ 3: This sends notifications about both incoming and outgoing traffic. The default is 0 (no notification).
ProtectionLevel=<value>	Determines the degree of protection that is provided by the firewall, where <value> is one of the following: ■ 0: Low ■ 1: Medium ■ 2: High ■ 3: Custom Low, Medium, and High levels are preconfigured for your convenience. If you are satisfied with the preconfigured settings, you don't need to set the Count parameter or write individual rules for incoming and outgoing services, or ICMP message types. Low uses the following parameter values: ■ LocalTrafficAllowed=1 (yes) ■ IGMPAllowed=0 (no) ■ TrafficNotifications=0 (none) ■ All inbound connections are allowed ■ All outbound connections are allowed ■ ICMP Echo Request is set to AllowOutgoing, and Echo Reply and Packet Too Big are set to AllowIncoming. Medium uses the same parameter values as Low, except that no inbound connections are allowed. High uses the same parameter values as Medium, with the following exceptions: ■ Only the following predefined outbound connections are enabled: FTP, IMAP3, IMAP4, SMTP, POP3, HTTPS, HTTP, and Telnet ■ TrafficNotifications=2 (outgoing) If you want to set the individual parameters yourself using the Count parameters and table values in your configuration input file, set the ProtectionLevel=3 (Custom) and set the counts for the services and ICMP message types that you want to configure individually. The default is 1 (Medium).

Table 6-5 Symantec Client Firewall general configuration parameters

FW section parameter	Description
Locked=<value>	Allow users to, or prevent users from, modifying firewall settings on the devices. ■ 0: Allow users to modify firewall settings on the devices. ■ 1: Do not allow users to modify firewall settings on the devices. The firewall user interface on the devices is locked. The default is 0 (allow modification).

Incoming services

The incoming services section of the ssb.ini file is used to configure local ports on the device. Incoming services enable inbound connections that are solicited from the device.

There are two kinds of incoming services, standard and user-defined. You can create as many user-defined services as you need on the device. It is unlikely that you would need to set incoming services individually on the device.

FW.IncomingSvcs section

Table 6-6 describes the Count parameter for the FW.IncomingSvcs section of the ssb.ini file, which is used to configure user-defined incoming services.

Table 6-6 FW.IncomingSvcs section parameter

FW.IncomingSvcs section parameter	Description
Count=<value>	Specifies the number of entries that you are configuring for user-defined incoming services. Incoming services configure local ports. There must be a property for each entry numbered 0 through count-1. Missing entries are flagged as an error. Duplicate entries are ignored, as is any entry with a value that is greater than or equal to count. Default is 0 (no user-defined incoming services configured).

Table 6-7 describes the format of user-defined service entries for inbound connections.

Table 6-7 User-defined incoming services entry format

FW.IncomingSvcs section number	Enabled/ Disabled/ Deleted	First port	Last port	Port type	Description
The count entry number	0=Disabled 1=Enabled 2=Delete Note: Delete disables the service and removes it from the device's user interface. Disabling a service simply dims that option on the device's user interface.	0-65535 To set a single port, set the first and last ports to the same number.	0-65535 This must be greater than or equal to the first port.	0=TCP 1=UDP	128 bytes, string This message appears in the user interface on the device. The message may not contain commas (,).

Table 6-8 gives examples of user-defined service entries for inbound connections.

Table 6-8 Sample user-defined incoming services entries

Number	Enabled/ Disabled/ Deleted	First port	Last port	Port type	Description
0=	1,	0,	100,	0,	“Service 100”
1=	1,	101,	200,	0,	“Service 200”

FW.InStdSvcs section

Table 6-9 describes the Count parameter for the FW.InStdSvcs section of the ssb.ini file, which is used to configure standard incoming services.

Table 6-9 FW.InStdSvcs section parameter

FW.InStdSvcs section parameter	Description
Count=<value>	Specifies the number of entries that you are configuring for standard incoming services. Incoming services configure local ports. There must be a property for each entry numbered 0 through count-1. Missing entries are flagged as an error. Duplicate entries are ignored, as is any entry with a value that is greater than or equal to count. Default is 0 (no incoming services configured).

Table 6-10 describes the format of standard service entries for inbound connections.

Table 6-10 Standard incoming services entry format

FW.InStdSvcs section number	Service ID	Enabled/Disabled

The count entry number	All_TCP=8
	All_UDP=9
		0=Disabled
		1=Enabled

Table 6-11 gives examples of standard service entries for inbound connections.

Table 6-11 Sample standard incoming services entries

Number	Service ID	Enabled/Disabled
0,	8,	1
1,	9,	0

Outgoing services

The outgoing services section of the ssb.ini file is used to configure connections to remote services. There are two kinds of outgoing services, standard and user-defined. You can create as many user-defined services as you need on the device.

FW.OutgoingSvcs section

Table 6-12 describes the Count parameter for the FW.OutgoingSvcs section of the ssb.ini file, which is used to configure user-defined outgoing services.

Table 6-12 FW.OutgoingSvcs section parameter

FW.OutgoingSvcs section parameter	Description
Count=<value>	Specifies the number of entries that you are configuring for user-defined outgoing services. Outgoing services configure remote ports. There must be a property for each entry numbered 0 through count-1. Missing entries are flagged as an error. Duplicate entries are ignored, as is any entry with a value that is greater than or equal to count. Default is 0 (no outgoing services configured).

Table 6-13 describes the format of entries for user-defined outgoing services.

Table 6-13 User-defined outgoing services entry format

FW.OutgoingSvcs section number	Enabled/Disabled/Deleted	First port	Last port	Port type	Description
The count entry number	0=Disabled 1=Enabled 2=Delete Note: Delete disables the service and removes it from the device's user interface. Disabling a service simply dims that option on the device's user interface.	0-65535 To set a single port, set the first and last ports to the same number.	0-65535 This must be greater than or equal to first port.	0=TCP 1=UDP	128 bytes, string This message appears in the user interface on the device. Note: The message may not contain commas (,).

Table 6-14 gives examples of entries for user-defined outgoing services.

Table 6-14 Sample user-defined outgoing services entries

Number	Enabled/ Disabled/ Deleted	First port	Last port	Port type	Description
0=	1,	800,	900,	0,	“My Service1“
1=	1,	500,	500,	0,	“My Service2“

FW.OutStdSvcs section

Table 6-15 describes the Count parameter for the FW.OutStdSvcs section of the ssb.ini file, which is used to configure standard outgoing services.

Table 6-15 FW.OutStdSvcs section parameter

FW.OutStdSvcs section parameter	Description
Count=<value>	Specifies the number of entries that you are configuring for standard outgoing services. Outgoing services configure remote ports. There must be a property for each entry numbered 0 through count-1. Missing entries are flagged as an error. Duplicate entries are ignored, as is any entry with a value that is greater than or equal to count. Default is 0 (no outgoing services configured).

Table 6-16 describes the format of entries for standard outgoing services.

Table 6-16 Standard outgoing services entry format

FW.OutStdSvcs section number	Service ID	Enabled/ Disabled
The count entry number	0=FTP 1=IMAP3 2=IMAP4 3=SMTP 4=POP3 5=HTTPS 6=Telnet 7=HTTP 8=All_TCP 9=All_UDP	0=Disabled 1=Enabled

Table 6-17 gives examples of entries for standard outgoing services.

Table 6-17 Sample standard outgoing services entries

Number	Service ID	Enabled/ Disabled
0,	0,	1
1,	1,	0
2,	8,	1
3,	9,	0

FW.ICMPMsgs section

Internet Control Message Protocol (ICMP) messages provide feedback about IP networks. For example, they can be used to verify that end systems or routers are operating correctly, or to report errors in processing IP datagrams.

Table 6-18 describes the Count parameter for the FW.ICMPMsgs section of the ssb.ini file, which is used to configure ICMP message type filtering.

Table 6-18 FW.ICMPMsgs section parameter

FW.ICMPMsgs section parameter	Description
Count=<value>	Specifies the number of entries that you are configuring for ICMP message service types. There must be a property for each entry numbered 0 through count-1. Missing entries are flagged as an error. Duplicate entries are ignored, as is as any entry with a value that is greater than or equal to count. Default is 0 (no ICMP message types configured).

The FW.ICMPMsgs section of the ssb.ini file describes the handling of each type of ICMP message. The State parameter in the entry determines the direction of the message's communication. Table 6-19 describes the format for ICMP message services. Elements in an entry are separated by commas.

Table 6-19 ICMP message services entry format

FW.ICMPMsgs section number	TypeV4	TypeV6	State
The count entry number.	See "ICMP message type values" on page 57.	See "ICMP message type values" on page 57.	0=DisallowAll 1=AllowIncoming 2=AllowOutgoing 3=AllowAll

Table 6-20 gives examples of entries for ICMP message types.

Table 6-20 Sample ICMP message types entries

Number	TypeV4	TypeV6	State
0=	0,	129,	1
1=	8,	128,	2
2=	-1,	2,	1

When configuring message type settings, keep in mind the following considerations:

- Use one entry for each message type that you want to configure.
- The appropriate ICMPv4 and ICMPv6 messages must be paired in each entry. If inappropriate messages are paired, an error message is generated to the console.
- You can configure entries for as many message types as you need.

Note: Once in place on the device, there is no way to delete these entries. You can, however, push a configuration file that sets the state of a message type entry to 0 (DisallowAll) to turn off that message's function on the device.

ICMP message type values

ICMP messages are identified by a type field. Symantec Client Security supports both ICMPv4 and ICMPv6 message numbers. Table 6-21 lists the allowed values for ICMPv4 and ICMPv6 message types when you use Symantec Settings Builder to configure the firewall. Use these values in the TypeV4 and TypeV6 columns of your ICMP message type entries.

Table 6-21 TypeV4 and TypeV6 message numbers

TypeV4 number	TypeV6 number	TypeV4 message; TypeV6 message
8	128	Echo Request
0	129	Echo Reply
3	1	Destination Unreachable
-1	2	Not supported; Packet Too Big
4	-1	Source Quench; Not Supported
5	137	Redirect
6	6	Alternate Host Address
9	134	Router Advertisement
10	133	Router Solicitation
11	3	Time Exceeded
12	4	Parameter Problem
13	13	Timestamp
14	14	Timestamp Reply
15	15	Information Request
16	116	Information Reply
17	17	Address Mask Request
18	18	Address Mask Reply
30	30	Trace Route
31	31	Datagram Conversion Error
32	32	Mobile Host Redirect
33	33	IPv6 Where-Are-You

Table 6-21 TypeV4 and TypeV6 message numbers

TypeV4 number	TypeV6 number	TypeV4 message; TypeV6 message
34	34	IPv6 I-Am-Here
35	35	Mobile Registration Request
36	36	Mobile Registration Reply
37	37	Domain Name Request
38	38	Domain Name Reply
39	39	SKIP Algorithm Discovery Protocol
40	40	Photuris
-1	130	Not Supported; Multicast Listener Query
-1	131	Not Supported; Multicast Listener Report
-1	132	Not Supported; Multicast Listenership
-1	135	Not Supported; Neighbor Solicitation
-1	136	Not Supported; Neighbor Advertisement
-1	138	Not Supported; Router Renumbering
-1	139	Not Supported; ICMP Node Information Query
-1	140	Not Supported; ICMP Node Information Response
-1	141	Not Supported; Inverse Neighbor Discovery Solicitation
-1	142	Not Supported; Inverse Neighbor Discovery Advertisement
-1	143	Not Supported; Home Agent Address Discovery Request
-1	144	Not Supported; Home Agent Address Discovery Reply
-1	145	Not Supported; Mobile Prefix Solicitation
-1	146	Not Supported; Mobile Prefix Advertisement

You can also find a listing of these message numbers, along with their associated RFC numbers, at www.iana.org, the Internet Assigned Numbers Authority Web site.

Using Symantec Settings Builder

Use Symantec Settings Builder to create the configuration files that you need to set and lock Symantec AntiVirus, Symantec Client Firewall, and LiveUpdate Wireless configuration settings on your devices.

Symantec Settings Builder command-line syntax is as follows:

```
ssb <config_file>
```

where <config_file> is the name of the input configuration file. The input file name may include a full or relative path.

The only command-line options for Symantec Settings Builder are /? and /h, which display the tool's Help text.

```
Symantec Client Security for Nokia Communicator, Version 3.0
Settings Builder.

Creates and packages configuration settings for Symbian OS devices
as specified by the input configuration file.

Usage:
SSB config_file
        [/?] [/h]

  config_file
    Input configuration file.  May include a full or relative path.

  /? or /h
    Displays this help text.
```

To use Symantec Settings Builder

1. Go to the directory where you copied the Symantec Settings Builder ssb.exe and sample ssb.ini files.
2. Copy the sample ssb.ini file and give it a new name, for example, my_config.ini.
3. Edit and save this file to set the Symantec AntiVirus, Symantec Client Firewall, and LiveUpdate Wireless configuration settings that you want.
4. At the command line, type:

   ```
   ssb my_config.ini
   ```

Depending on how you edited your version of the .ini file, this produces one or more of the following files:

av.cfg	Symantec AntiVirus configuration file for configuring Symantec Client Security on the device
lu.cfg	LiveUpdate Wireless configuration file for configuring Symantec Client Security on the device
fw.cfg	Firewall configuration file for configuring Symantec Client Security on the device

The files are placed in the directory specified by your OutputDir parameter.

If you set configuration parameters for Symantec AntiVirus, LiveUpdate Wireless, and Symantec Client Firewall, you see output similar to the following:

```
Creating AntiVirus configuration.
Creating LiveUpdate configuration.
Creating Firewall configuration.
```

Troubleshooting configuration files

The configuration files are created by Symantec Settings Builder in the following order:

- av.cfg
- lu.cfg
- fw.cfg

If you use an invalid entry in your input configuration file, Symantec Settings Builder generates an error message to the console and stops creating output files. For example, if you set it to produce all of the configuration files, but you set the Enabled parameter for LiveUpdate Wireless to equal 3 (which is an invalid entry), Symantec Settings Builder will produce the av.cfg file and then stop.

Note: When you run Symantec Settings Builder, you see any validation error messages that are generated on the console regardless of whether the Verbose parameter is set to 1.

Transferring configuration files to the devices

Symantec Settings Builder configuration files are designed to be used with the administrator's existing infrastructure to transfer update and configuration files to the devices.

The existing infrastructure that administrators use to transfer update and configuration files must be configured as follows:

- To place the configuration files in specific locations on the device.
- To invoke the proper configuration executable for each file to ensure that the file takes effect on the device.

Required file locations

The existing infrastructure that administrators use to transfer update and configuration files must be configured to place the Symantec Client Security configuration files on the device in the locations that are shown in Table 6-22.

Table 6-22 Required configuration file locations

Configuration file	Device directory
av.cfg, fw.cfg	C:\System\Apps\SymCS
lu.cfg	C:\System\Apps\SymLU

Configuration executables

The existing infrastructure that administrators use to transfer configuration files must invoke the proper configuration executable for each file to ensure that the file takes effect on the device. The configuration executables are installed on the device in the correct location when you initially install Symantec Client Security on the devices. Configuration executables and their locations are listed in Table 6-23.

Table 6-23 Configuration executables

Configuration file	Configuration executable
av.cfg	C:\System\Apps\SymCS\avcfg.exe
fw.cfg	C:\System\Apps\SymCS\fwcfg.exe
lu.cfg	C:\System\Apps\SymLU\lucfg.exe

Once the files are transferred to the device and the configuration executables are invoked, the new configurations take effect.

Testing a new configuration

You should always push the configuration files that are produced by Symantec Settings Builder to at least one device and check to see that the parameters you set have the desired effect on the device before you deploy them to multiple devices.

How you test your configuration depends on the parameters that you set, but in general, it is good practice to push the files to a device, and then check at least one parameter that you set for each of the components (Symantec AntiVirus, LiveUpdate Wireless, and Symantec Client Firewall).

For Symantec AntiVirus, you should check that the Auto-Protect setting is as you set it in the file. For LiveUpdate Wireless, you can check that it is enabled or disabled, as you set it in the file. If you set it to use an internal LiveUpdate server, run a LiveUpdate Wireless session from the device to ensure that the updates download.

In the case of the firewall, you'll need to initiate traffic that should be stopped and traffic that should go through to see if your configuration gives the expected results. For example, if you've set traffic notifications to 3 (both incoming and outgoing), check to see that traffic alerts appear on the device screen.

Best practices when configuring components

The best practices for configuring devices are as follows:

- Keep Auto-Protect enabled.
- Keep the firewall enabled, with the protection level set to at least Medium.
- Configure your email server to block or remove messages that contain file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr files.

If you customize your firewall settings, you should do the following:

- Enable the following communication protocols:
  - HTTP
  - HTTPS
- Enable the email protocol that your organization uses:
  - IMAP3
  - IMAP4
  - SMTP
  - POP3
- Enable the following protocols if required:
  - Telnet
  - FTP

Index

A

Activity Log
- about 14, 15, 17, 28
- firewall activities 16, 29
- how activities are logged 16
- virus activities 16, 29

administration tool. *See* Symantec Settings Builder

antivirus events, logging 16, 29

application operation parameters 42

Auto-Protect, about 26

AV section parameters, ssb.ini file 43

av.cfg 40, 60, 61

avcfg.exe 61

C

CommandID
- command-line program 38
- SMS message 36

configuration executables 61

configuration files
- about 40
- testing 62
- transferring to devices 61
- troubleshooting 60

configuration tool. *See* Symantec Settings Builder

E

EICAR test file 23

F

firewall
- about configuration 46
- logging activities 16, 29
- parameters
  - example 48
  - general 48
  - incoming services 50
  - outgoing services 52
- stateful inspection 47

FW section parameters, ssb.ini file 48

fw.cfg 40, 60, 61

FW.ICMPMsgs section parameters, ssb.ini file 55

FW.IncomingSvcs section parameters, ssb.ini file 50

FW.InStdSvcs section parameters, ssb.ini file 52

FW.OutgoingSvcs section parameters, ssb.ini file 53

FW.OutStdSvcs section parameters, ssb.ini file 54

fwcfg.exe 61

I

installation
- administration tool files 21
- device system requirements 20
- on the devices 21
- Symantec Settings Builder system requirements 20
- testing 23
- uninstallation 23

L

LiveUpdate Wireless
- about 13, 15, 17
- parameters 44
- software updates 15
- virus definitions files updates 15

LU section parameters, ssb.ini file 44

lu.cfg 40, 60, 61

lucfg.exe 61

P

ports
- about scanning attempts 15, 16, 17, 29
- Destination Port 29
- HTTP 32, 47
- HTTPS 47
- incoming services 50
- local 50
- outbound rules 47

ports *(continued)*
- remote 53
- SMS messaging 35, 36, 37
- Source Port 29
- stateful inspection 47
- Symantec private port 35
- Telnet 47

R

remote operations, initiating 37

S

scans
- Auto-Protect 14, 16, 26
- compressed files 26
- initiating remotely 27
- on-demand 15

Short Message Service Listener, about 35

SMS message
- CommandID 36
- format 36
- payload format 36

SSB section parameters, ssb.ini file 42

ssb.ini
- about the sample file 40
- AV section parameters 43
- FW section parameters 48
- FW.ICMPMsgs section parameters 55
- FW.IncomingSvcs section parameters 50
- FW.InStdSvcs section parameters 52
- FW.Outgoing.Svcs section parameters 53
- FW.OutStdSvcs section parameters 54
- LU section parameters 44
- SSB section parameters 42

stateful inspection, firewall 47

Symantec AntiVirus
- configuration parameters 43
- software 13

Symantec Client Firewall 13

Symantec Settings Builder
- about 39, 59
- command line options 59
- parameters
  - application operation 42
  - firewall 48
  - LiveUpdate Wireless 44
  - Symantec AntiVirus configuration 43
- producing configuration files 59

Symantec Settings Builder *(continued)*
- sample .ini file 40
- system requirements 20
- troubleshooting configuration files 60
- using 59

system requirements
- for the devices 20
- Symantec Settings Builder 20

U

uninstallation 23

updates
- LiveUpdate Wireless
  - using internal server 32
  - using Internet 32
- software 31
- virus definitions files 31

V

viruses
- allowing 26
- deleting 26
- denying access 26
- logging virus activities 14, 15, 16, 29